CHAPTER TWENTY-FIVE

Voting system ☆

Shubhani Aggarwal and Neeraj Kumar
Thapar Institute of Engineering & Technology, Patiala, Punjab, India

Contents

1. Current digital voting system 496
2. Blockchain-based online voting system 496
   2.1 Record-keeping database or database manipulation 497
   2.2 Tamper-proof vote counting 498
References 499
About the authors 499

Abstract

This chapter aims to solve the issues of the digital voting process using blockchain technology. Firstly, introducing the problems in the current voting system then goes into a brief explanation of blockchain technology that how it is currently being used in the digital voting process. This chapter represents the digital voting process in detail and the issues they face. Here, we represent the blockchain-based platform to the voting system that ensures the privacy of the voter's vote. This platform also provides data immutability and transparency to the digital voting process.

Chapter points

- In this chapter, we discuss the role of blockchain in the voting system.
- Here, we discuss the changes made in the traditional voting system after using blockchain technology.

Democratic voting is a very crucial and serious event in any country. The most common way of voting is through a paper-based system, but this is not time to vote using a paper into the 21st century of this modern world. The digital voting process is the use of electronic devices, such as voting machines, Internet browsers, to cast voters to vote. This is also known as e-voting system or an online voting system.

The major concern of the digital voting process is the security and privacy of the votes. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against

☆ Applications.

Advances in Computers, Volume 121
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2020.08.025

© 2021 Elsevier Inc.
All rights reserved.

potential attacks. The only solution is the blockchain technology that can be potentially solved the issues of the digital voting system. It is a form of a distributed database where records stored in the form of transactions in a block. With the use of blockchain technology, a secure and robust platform for the digital voting system can be provided.

1. Current digital voting system

Several countries are currently using digital voting systems around the world. For example, Estonia has had the electronic voting system since 2005 and in 2007 was the first country in the world, which allows the online voting system to cast the votes at their respective places. The bases of this system are the national ID card that all Estonian citizens are given. These cards contain encrypted files that identify the owner and allows the owner to carry out online and electronic activities including online banking services, digitally signing documents, access their information on government databases, and e-voting [1].

To cast a vote in an online system, the voter should enter their card number into a card reader and then access the voting website on the computer. Then, the voter enters the PIN number and an online system checks that the voter is eligible to vote or not. Once confirmed, the voter can cast the vote on election day. The voter can also use a mobile phone to cast a vote in an online voting system. When the voter submits its vote, a vote is passed through the publicly accessible server to the vote storage server where it is encrypted and stored until the online voting process is over. Then, the vote has all identifying information cleaned from it and is transferred by DVD to a vote counting server which is disconnected from all networks. This server decrypts and counts the votes and then outputs the results. Each stage of this process is logged and audited [2]. In this process, there is the possibility of risks via malware on the client-side machine that monitors the user placing their vote and then later changing the votes to a different candidate. The other possible risk is for an attacker to directly infect the servers though malware being placed on the DVDs used to set up the servers and transfer the votes [3].

The scenario of online voting system in Estonia [1] is as shown in Fig. 1.

2. Blockchain-based online voting system

The traditional and online electoral systems have to handle many issues and problems related to security, privacy, and transparency in its

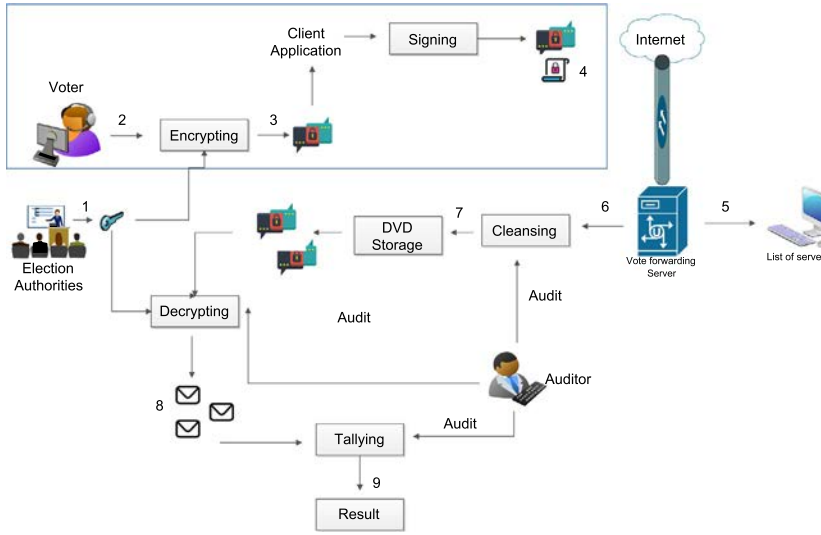

Fig. 1 Online voting system in Estonia [1].

existing manner of execution. Electoral systems use a centralized network wherein all the processing is handled by a trusted third party. However, this leads to some other major concerns in the form of security and transparency in these systems. To solve these problems in the online voting system, blockchain technology is a promising solution. It not only authenticates the voters but also provides confidentiality of the votes in online voting system. The architecture of the blockchain-based voting process system is as shown in Fig. 2. In this architecture, blockchain safeguards and secures the entire voter registration, voting, and counting processes in a distributed manner.

The usage of blockchain in the online voting system in two aspects, which is described as follows.

2.1 Record-keeping database or database manipulation

In an online voting process, the prevention of voting database manipulation is of utmost importance. Moreover, the manipulation in the result voting data is also an important concern. The use of blockchain technology with permission protocol provides a distributed record-keeping framework to an online voting system. It uses SHA-256 to compute the hash values for recording the voting results of different stations that are linked to each other. The use of digital signatures having blockchain in the voting system provides

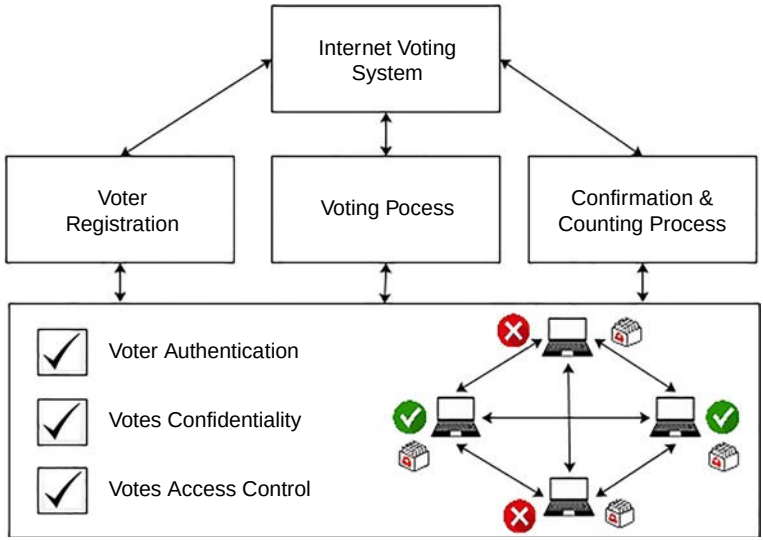

Fig. 2 Blockchain in online voting system.

reliability to the system. Hence, by integrating the blockchain in the online voting system ensures decentralized, non-interactive, self-managed, and free receipt platform for a large scale electoral process [4,5]

2.2 Tamper-proof vote counting

Vote counting in the online voting process must be tamper-proof and secure in every manner. An attacker can gain control of the counting process and manipulate the votes and alter the winning candidate, which may lead to serious obligations. The verifiability process of blockchain in the online voting system provides a reliable, verifiable, transparent, secure, and efficient platform [6].

In the end, it has been observed that the blockchain technology provides transparent, tamper-proof, and reliable results in the online voting process. To ensure a secure voting process, the private blockchain platform can be used in which nodes will behave in a restricted manner. In this network, every node cannot participate in the blockchain and there is strict authority management on data access. It would establish more trust and thereby encourage more people participation and vote in the democratic process. But in addition to this, blockchain technology is the biggest challenge for those countries which have low Internet connectivity and mobile penetration.

References

[1] Valimised, Available: https://www.valimised.ee/et (accessed 10 May 2020).
[2] E-voting is (too) secure, Available: https://www.ria.ee/en/news/e-voting-too-secure.html (accessed 10 May 2020).
[3] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, J.A. Halderman, Security analysis of the Estonian internet voting system, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 703–715.
[4] R. Hanifatunnisa, B. Rahardjo, Blockchain based e-voting recording system design, in: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), IEEE, 2017, pp. 1–6.
[5] B. Wang, J. Sun, Y. He, D. Pang, N. Lu, Large-scale election based on blockchain, Procedia Comput. Sci. 129 (2018) 234–237.
[6] S.H. Shaheen, M. Yousaf, M. Jalil, Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain, in: 2017 13th International Conference on Emerging Technologies (ICET), IEEE, 2017, pp. 1–6.

About the authors

Shubhani Aggarwal is pursuing a PhD from Thapar Institute of Engineering and Technology (Deemed to be University), Patiala, Punjab, India. She received the BTech degree in Computer Science and Engineering from Punjabi University, Patiala, Punjab, India, in 2015, and the ME degree in Computer Science from Panjab University, Chandigarh, India, in 2017. She has many research interests in the area of Blockchain, cryptography, Internet of Drones, and information security.

Neeraj Kumar received his PhD in CSE from Shri Mata Vaishno Devi University, Katra (Jammu and Kashmir), India in 2009, and was a postdoctoral research fellow in Coventry University, Coventry, UK. He is working as a professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology (Deemed to be University), Patiala (Pb.), India. He has published more than 400 technical research papers in top-cited journals such as IEEE TKDE, IEEE TIE, IEEE TDSC, IEEE TITS, IEEE TCE, IEEE TII, IEEE TVT, IEEE ITS, IEEE SG, IEEE Netw., IEEE Comm., IEEE WC, IEEE IoTJ, IEEE

SJ, Computer Networks, Information sciences, FGCS, JNCA, JPDC, and ComCom. He has guided many research scholars leading to PhD and ME/MTech. His research is supported by funding from UGC, DST, CSIR, and TCS. His research areas are Network Management, IoT, Big Data Analytics, Deep Learning, and Cybersecurity. He is serving as editors of the following journals of repute: ACM Computing Survey, ACM·IEEE Transactions on Sustainable Computing, IEEE·IEEE Systems Journal, IEEE·IEEE Network Magazine, IEE·IEEE Communication Magazine, IEE·Journal of Networks and Computer Applications, Elsevier·Computer Communication, Elsevier·International Journal of Communication Systems, Wiley. Also, he has been a guest editor of various International Journals of repute such as—IEEE Access, IEEE ITS, Elsevier CEE, IEEE Communication Magazine, IEEE Network Magazine, Computer Networks, Elsevier, Future Generation Computer Systems, Elsevier, Journal of Medical Systems, Springer, Computer and Electrical Engineering, Elsevier, Mobile Information Systems, International Journal of Ad hoc and Ubiquitous Computing, Telecommunication Systems, Springer and Journal of Supercomputing, Springer. He has also edited/authored 10 books with International/National Publishers like IET, Springer, Elsevier, CRC. Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions (ISBN-13: 978-1-78561-898-7), Machine Learning for cognitive IoT, CRC Press, Blockchain, Big Data and IoT, Blockchain Technologies across industrial vertical, Elsevier; Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms and Solutions (ISBN: 978-981-13-8759-3), Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019) (ISBN 978-981-15-3369-3). One of the edited text-book entitled, "Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms, and Solutions" published in Springer in 2019 is having 3.5 million downloads till 6 June, 2020. It attracts attention of the researchers across the globe (https://www.springer.com/in/book/9789811387586). He has been a workshop chair at IEEE Globecom 2018 and IEEE ICC 2019 and TPC Chair and member for various International conferences such as IEEE MASS 2020, IEEE MSN2020. He is senior member of the IEEE. He has more than 12,321 citations to his credit with current h-index of 60 (September 2020). He has won the best papers award from IEEE Systems Journal and ICC 2018, Kansas-city in 2018. He has been listed in the highly cited researcher of 2019 list of web of science (WoS). In India, he is listed in top 10 position among highly cited researchers list. He is adjunct professor at Asia University, Taiwan, King Abdul Aziz University, Jeddah, Saudi Arabia and Charles Darwin University, Australia.